Contents

An Automata-Theoretic Approach to Modeling Systems and Specifications over Infinite Data .................................................. 1
   Hadar Frenkel, Orna Grumberg, and Sarai Sheinvald

Learning from Faults: Mutation Testing in Active Automata Learning ........ 19
   Bernhard K. Aichernig and Martin Tappler

Parametric Model Checking Timed Automata Under
Non-Zenoness Assumption ...................................................... 35
   Étienne André, Hoang Gia Nguyen, Laure Petrucci, and Jun Sun

Multi-timed Bisimulation for Distributed Timed Automata .................. 52
   James Ortiz, Moussa Amrani, and Pierre-Yves Schobbens

Auto-Active Proof of Red-Black Trees in SPARK ............................. 68
   Claire Dross and Yannick Moy

Analysing Security Protocols Using Refinement in iUML-B ................... 84
   Colin Snook, Thai Son Hoang, and Michael Butler

On Learning Sparse Boolean Formulae for Explaining AI Decisions ........... 99
   Susmit Jha, Vasumathi Raman, Alessandro Pinto, Tuhin Sahai,
   and Michael Francis

Event-Based Runtime Verification of Temporal Properties
Using Time Basic Petri Nets .................................................. 115
   Matteo Camilli, Angelo Gargantini, Patrizia Scandurra,
   and Carlo Bellettini

Model-Counting Approaches for Nonlinear Numerical Constraints .......... 131
   Mateus Borges, Quoc-Sang Phan, Antonio Filieri,
   and Corina S. Păsăreanu

Input Space Partitioning to Enable Massively Parallel Proof ................. 139
   Ashlie B. Hocking, M. Anthony Aiello, John C. Knight,
   and Nikos Arêchiga

Compositional Model Checking of Interlocking Systems for Lines
with Multiple Stations ....................................................... 146
   Hugo Daniel Macedo, Alessandro Fantechi, and Anne E. Haxthausen
Modular Model-Checking of a Byzantine Fault-Tolerant Protocol ............................................ 163
    Benjamin F. Jones and Lee Pike

Improved Learning for Stochastic Timed Models by State-Merging Algorithms ........................................ 178
    Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, and Saddek Bensalem

Verifying Safety and Persistence Properties of Hybrid Systems Using Flowpipes and Continuous Invariants .................... 194
    Andrew Sogokon, Paul B. Jackson, and Taylor T. Johnson

A Relational Shape Abstract Domain ................................................................. 212
    Hugo Illous, Matthieu Lemerre, and Xavier Rival

Floating-Point Format Inference in Mixed-Precision ................................................................. 230
    Matthieu Martel

A Verification Technique for Deterministic Parallel Programs ........................................ 247
    Saeed Darabi, Stefan C.C. Blom, and Marieke Huisman

Systematic Predicate Abstraction Using Variable Roles ......................................................... 265
    Yulia Demyanova, Philipp Rümmer, and Florian Zuleger

specgen: A Tool for Modeling Statecharts in CSP ......................................................... 282
    Brandon Shapiro and Chris Casinghino

HyPRO: A C++ Library of State Set Representations for Hybrid Systems Reachability Analysis ........................................... 288
    Stefan Schupp, Erika Ábrahám, Ibtissem Ben Makhlouf, and Stefan Kowalewski

Asm2C++: A Tool for Code Generation from Abstract State Machines to Arduino ......................................................... 295
    Silvia Bonfanti, Marco Carissoni, Angelo Gargantini, and Atif Mashkoor

SPEN: A Solver for Separation Logic ................................................................. 302
    Constantin Enea, Ondřej Lengál, Mihaela Sighireanu, and Tomáš Vojnar

From Hazard Analysis to Hazard Mitigation Planning: The Automated Driving Case ........................................... 310
    Mario Gleirscher and Stefan Kugele

Event-B at Work: Some Lessons Learnt from an Application to a Robot Anti-collision Function ........................................... 327
    Arnaud Dieumegard, Ning Ge, and Eric Jenn
Reasoning About Safety-Critical Information Flow Between Pilot and Computer. .......................... 342
  Seth Ahrenbach

Compositional Falsification of Cyber-Physical Systems with Machine Learning Components .................... 357
  Tommaso Dreossi, Alexandre Donzé, and Sanjit A. Seshia

Verifying a Class of Certifying Distributed Programs. .................. 373
  Kim Völlinger and Samira Akili

Compact Proof Witnesses. ........................................ 389
  Marie-Christine Jakobs and Heike Wehrheim

Qualification of a Model Checker for Avionics Software Verification ........ 404
  Lucas Wagner, Alain Mebsout, Cesare Tinelli, Darren Cofer, and Konrad Slind

SpeAR v2.0: Formalized Past LTL Specification and Analysis of Requirements .................................................. 420
  Aaron W. Fifarek, Lucas G. Wagner, Jonathan A. Hoffman, Benjamin D. Rodes, M. Anthony Aiello, and Jennifer A. Davis

Just Formal Enough? Automated Analysis of EARS Requirements .......... 427
  Levi Lúcio, Salman Rahman, Chih-Hong Cheng, and Alistair Mavin

Author Index .......................................................... 435
NASA Formal Methods
9th International Symposium, NFM 2017, Moffett Field, CA, USA, May 16-18, 2017, Proceedings
Barrett, C.; Davies, M.; Kahsai, T. (Eds.)
2017, XI, 436 p. 124 illus., Softcover
ISBN: 978-3-319-57287-1